NEW YORK STATE SECURITY BREACH REPORTING FORM

Pursuant to the Information Security Breach and Notification Act

(General Business Law §899-aa)

Name and address of Entity that owns or licenses the computerized data that was subject to the breach:
Jenner & Block LLP
Street Address: 353 North Clark Street,
City: Chicago State: IL Zip Code: 60654

Submitted by: Mary Ellen Callahan Title: Partner Dated: 2/9/2017
Firm Name (if other than entity):
Telephone: 202 639 6064 Email: mecallahan@jenner.com
Relationship to Entity whose information was compromised: Partner

Type of Organization (please select one): [ ] Governmental Entity in New York State; [ ] Other Governmental Entity; [ ] Educational; [ ]Health Care; [ ]Financial Services; [X]Other Commercial; or [ ]Not-for-profit.

Number of Persons Affected:
Total (Including NYS residents): 859 NYS Residents: 88
If the number of NYS residents exceeds 5,000, have the consumer reporting agencies been notified? [ ] Yes [ ] No

Dates: Breach Occurred: 2/2/2017 Breach Discovered: 2/6/2017 Consumer Notification: 2/10/2017

Description of Breach (please select all that apply):
[ ]Loss or theft of device or media (e.g., computer, laptop, external hard drive, thumb drive, CD, tape);
[ ]Internal system breach; [ ]Insider wrongdoing; [ ]External system breach (e.g., hacking);
[X]Inadvertent disclosure ; [ ]Other specify):

Information Acquired: Name or other personal identifier in combination with (please select all that apply):
[X]Social Security Number
[ ]Driver's license number or non-driver identification card number
[ ]Financial account number or credit or debit card number, in combination with the security code, access code, password, or PIN for the account

Manner of Notification to Affected Persons - ATTACH A COPY OF THE TEMPLATE OF THE NOTICE TO AFFECTED NYS RESIDENTS:
[X] Written [ ] Electronic [ ] Telephone [ ] Substitute notice
List dates of any previous (within 12 months) breach notifications:

Identify Theft Protection Service Offered: [X]Yes [ ] No
Duration: 2 years Provider: Experian
Brief Description of Service: ProtectMyID Elite 3B

PLEASE COMPLETE AND SUBMIT THIS FORM TO
EACH OF THE THREE STATE AGENCIES LISTED BELOW:

Fax or Email this form to:

New York State Attorney General's Office
SECURITY BREACH NOTIFICATION
Consumer Frauds & Protection Bureau
120 Broadway - 3rd Floor
New York, NY 10271
Fax: 212-416-6003
Email: breach.security@ag.ny.gov

New York State Division of State Police
SECURITY BREACH NOTIFICATION
New York State Intelligence Center
31 Tech Valley Drive, Second Floor
East Greenbush, NY 12061
Fax: 518-786-9398
Email: risk@nysic.ny.gov

New York State Department of State Division of Consumer Protection
Attention: Director of the Division of Consumer Protection
SECURITY BREACH NOTIFICATION
99 Washington Avenue, Suite 650
Albany, New York *12231*
Fax: (518) 473-9055
Email: security_breach_notification@dos.ny.gov

353 N. CLARK STREET CHICAGO, IL 60654-3456

JENNER & BLOCK LLP

February 9, 2017

Brent E. Kidwell
Tel +1 312 923 2794
BKidwell@jenner.com

«Full_Name»
«Address1»
«Address2»
«City», «ST» «Zip»

Subject: Notice of Jenner & Block Employee Data Incident. After reading this entire letter, if you have any questions, please contact Experian at 877-441-6943.

Dear «First»:

Jenner & Block LLP has become the victim of an email phishing incident that resulted in disclosure of the information on its current and former employees' 2016 IRS W-2 forms. This incident affects only current and former employees who received a Form W-2 from Jenner & Block for 2016. You are receiving this letter because our records show that you received a Form W-2 from Jenner & Block for 2016.

What Happened:

The incident occurred on Thursday, February 2, 2017, and firm management learned of it late in the afternoon of February 6, 2017. A file containing the 2016 IRS Forms W-2 for Jenner & Block LLP current and former employees was mistakenly transmitted to an unauthorized recipient in response to what was believed to be a legitimate request from management. The incident only involved employee Form W-2 information and did not involve any other employee information, or information relating to any dependents or family members of current or former employees.

What Information Was Involved:

W-2 forms contain an employee's name, address, Social Security number, and income and tax information.

What We Are Doing:

Jenner & Block is providing all affected current and former employees with complimentary Experian Fraud Resolution assistance and a complimentary two-year membership to Experian's ProtectMyID® Elite 3B.

Fraud Resolution through Experian is available immediately and for two years from the date of this letter, even if you do not enroll in the credit monitoring service. Fraud Resolution does not require any action on your part at this time.

As stated, we are also offering fraud detection tools through ProtectMyID® Elite 3B, which does require enrollment, but is of no cost to you and does not require you to provide a credit card or purchase any other products. This product monitors your credit accounts for fraud and provides you with identity detection and resolution of identity theft. Enclosed you will find information on how to begin credit monitoring, including an engagement number and your unique enrollment code. **Please retain this information; you will need it to register for services.**

Please note that we cannot enroll you in these services. You must register yourself. Enclosed please find additional information in the Frequently Asked Questions section of this letter.

What You Can Do:

It is always important to remain vigilant and monitor your financial account statements and credit reports for signs of fraud. There are also a number of steps you can take to protect yourself, such as placing a freeze or fraud alert on your credit report; filing an identity theft affidavit with the IRS; or contacting the appropriate authorities if you believe you have been the victim of identity theft. The enclosed "Identity Theft Protection Tips" and Frequently Asked Questions explain how you can take some of these steps.

Because your W-2 was affected, someone could file a fraudulent tax return using your Social Security number now or in the future. If you haven't filed taxes for 2016 and no other return has been submitted in your name, the IRS recommends you file your taxes electronically, even if your data is not complete or it contains errors. You can correct any errors in that return with an amended filing at a later date. Filing an electronic return quickly may prevent someone else (who wants to misuse your information) from taking your allocated "slot" in the IRS e-file system.

You can also consider submitting an IRS Form 14039, Identity Theft Affidavit, which results in the IRS marking an account for questionable activity. If you have filed your federal tax return for 2016, you can still submit an IRS Form 14039, Identity Theft Affidavit, in order to protect yourself in the future. Please note that submitting the IRS Form 14039 may require you to submit a paper tax return in the future, rather than filing electronically.

Other Important Information:

If you believe you are the victim of identity theft, you should contact your local law enforcement and file a police report. For additional information, view the enclosed "Identity Theft Protection Tips."

For More Information:

If you have any questions about enrolling in the credit monitoring service or the services provided, please contact Experian at 877-441-6943. If you have any additional questions for Jenner & Block after reviewing this letter and the enclosed Frequently Asked Questions, you can also contact the hotline we have established regarding this issue at 312-923-2666.

Sincerely,

Brent E. Kidwell
Chief Information Security Officer

Attachments: Experian ProtectMyID® Elite 3B Activation Information
Identity Theft Protection Tips
Frequently Asked Questions

Fraud Resolution and Credit Monitoring

FRAUD RESOLUTION ASSISTANCE

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that fraud resolution support is needed then an Experian Fraud Resolution agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition.)

Please note that this offer is available to you for two years from the date of this letter and does not require any action on your part at this time.

The Terms and Conditions for this offer are located at www.experian.com/fraudresolution. You will also find self-help tips and information about identity protection at this site.

CREDIT MONITORING ENROLLMENT

While Fraud Resolution assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through **ProtectMyID® Elite** as a **complimentary two-year membership**. This product provides you with identity detection services and resolution of identity theft. To start monitoring your personal information please follow the steps below:

1. Visit the ProtectMyID website to enroll: **www.protectmyid.com/enroll**
2. Provide your activation code: **«ExpCode»**
3. Ensure that you **enroll by February 16, 2019** (Your code will not work after this date.)

ProtectMyID Membership Additional Details

- A credit card is **not** required for enrollment in ProtectMyID.
- You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in ProtectMyID:
    - **Experian credit report at signup:** See what information is associated with your credit file.
    - **Active Surveillance Alerts:** Monitors Experian, Equifax and Transunion files for indicators of fraud.
    - **Internet Scan:** Alerts you if your information is found on sites containing compromised data.
    - **Address Change Alerts:** Alerts you of changes to your mailing address.
    - **Fraud Resolution:** Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.

- **ExtendCARE**: You receive the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.
- **Lost Wallet Protection:** Get help replacing credit, debit, and medical insurance cards.

If you have questions about the service, need assistance with fraud resolution that arose as a result of this incident or would like an alternative to enrolling in ProtectMyID online, please contact Experian's customer care team at 877-441-6943 by **February 16, 2019**. Be prepared to provide engagement number – [redacted] – as proof of eligibility for the fraud resolution services by Experian.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*

Identity Theft Protection Tips

You should consider taking the following steps to protect yourself and your identity:

- **Enroll in ProtectMyID® Elite 3B.** As explained above, Jenner & Block is providing you pre-paid, two-year membership for credit monitoring from Experian. See the enclosed information regarding how to activate your membership. Please note that the activation code provided is specific to you and should not be shared with anyone. Please note also that only you can activate your membership. We cannot activate this product on your behalf.

- **Place a security freeze or fraud alert on credit files.** State laws permit you to place a security freeze on your credit files. The purpose of a freeze is to prevent credit cards, loans, or other forms of credit from being opened in your name without your permission by restricting access to your credit report. Depending on the applicable state laws, there may be a small charge for placing a freeze on your credit file.

  You may also elect to place a fraud alert on your credit files. A fraud alert notifies lenders that you may be the victim of identity theft and requires them to take certain verification procedures before opening new accounts in your name.

  For more information about placing a security freeze or fraud alert on your credit file, contact the following credit reporting agencies:

Equifax	**Experian**	**TransUnion**
PO Box 740256	PO Box 9554	PO Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
888-766-0008	888-397-3742	800-680-7289

- **Vigilantly monitor your credit files, bank account statements, credit card statements, etc. closely for indications of identity theft or other misuse.**

- **What you can do to protect your information:** There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.experian.com/fraudresolution for this information.

If you believe you are the victim of identity theft, you should contact your local law enforcement and file a police report. You should also consider contacting the U.S. Federal Trade Commission's identity theft hotline at (877) 438-4338, or www.ftc.gov/idtheft to file a report and to obtain more information about combating identity theft. You may also wish to contact your state Attorney General. Maryland residents can contact their AG at: (410) 576-6566; North Carolina residents can contact their AG at: (919) 716-6000; contact information for the other Attorneys General is available at: http://www.naag.org/current-attorneys-general.php. The FTC and your state Attorney General can also provide you with additional information on how to protect yourself from identity theft.

CONFIDENTIAL

JENNER & BLOCK INCIDENT

Jenner & Block has become the victim of an email phishing incident that resulted in disclosure of the information on its employees' 2016 IRS W-2 forms. This incident affects only employees who received a Form W-2 from Jenner & Block for 2016 and you will not be affected if you did not receive a Form W-2. If you have received a Form W-2 for 2016, please immediately review the information in the Frequently Asked Questions below.

Jenner & Block is providing all affected employees with complimentary Experian Fraud Resolution assistance and a complimentary two year membership to ProtectMyID® Elite 3B (more details below). The fraud resolution assistance is available to you immediately, even if you do not enroll in the credit monitoring service.

FREQUENTLY ASKED QUESTIONS

Q1: What happened?
A1: Jenner & Block has become the victim of an email phishing incident that resulted in disclosure of 2016 W-2 information of its current and former employees. On February 2, 2017, a file containing the 2016 IRS Form W-2 for Jenner & Block LLP employees was mistakenly transmitted to an unauthorized recipient in response to what was believed to be a legitimate request from management.

Q2: What can I do to protect myself?
A2: Jenner & Block is providing all affected employees with complimentary Experian Fraud Resolution assistance and a complimentary two year membership to Experian's ProtectMyID® Elite 3B. The fraud resolution assistance is available to you immediately, even if you do not enroll in the credit monitoring service.

You will receive a formal notification and further instruction by U.S. postal mail within the next week, including how to enroll in two years of complimentary credit monitoring through ProtectMyID® Elite. Please note that we cannot enroll you in the services. You must register yourself.

In the meantime, you should remain vigilant and monitor your financial accounts. You should consider taking some additional steps to protect against identity theft and fraud, including:

- **Obtain a free copy of your credit report:** You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

- **Consider placing a security freeze or fraud alert on credit files:** State laws permit you to place a security freeze on your credit files. The purpose of a freeze is to prevent credit cards, loans, or other forms of credit from being opened in your name without your permission by restricting access to your credit report. Depending on the applicable state laws, there may be a small charge for placing a freeze on your credit file. **Note that if you place a security freeze on your files it will also make it more difficult for you to open new lines of credit in your name.**

Alternatively, you may also elect to place a fraud alert on your credit files. There are two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax:	1-888-766-0008, www.equifax.com
Experian:	1-888-397-3742, www.experian.com
TransUnion:	1-800-680-7289, fraud.transunion.com

- **Consider Submitting an IRS Form 14039, Identity Theft Affidavit:** If you have filed your federal tax return for 2016, you can still submit an IRS Form 14039, Identity Theft Affidavit, in order to protect yourself in the future.

  If a fraudulent return already has been electronically filed in your name, you must:
  - File a paper tax return with a completed IRS Form 14039, Identity Theft Affidavit. The IRS recommends that you attach that form to the front of the paper return.
  - The IRS has indicated that it may take up to six months to process the valid tax return you filed after a fraudulent return was also filed.

- **If Someone Has Already Filed a Tax Return Fraudulently in Your Name, Obtain an Electronic Filing PIN from the IRS:** Because your W-2 was affected, someone could file a fraudulent tax return using your Social Security number now or in the future. If you try to file your tax return and receive a message that you have already filed for 2016, you should obtain from the IRS an Electronic Filing PIN. The PIN may not protect your 2016 return, but it will provide protection for future filings.

  Visit https://www.irs.gov/individuals/get-an-identity-protection-pin or call 800-908-4490 and follow the system prompts. If an accountant or tax preparer files your return on your behalf, he or she may have a PIN for you. Be sure to discuss this incident with your tax preparer.

- **If you haven't filed taxes for 2016 and no other return has been submitted in your name, the IRS recommends you file your taxes electronically, even if your data is not complete or it contains errors.** You can correct any errors in that return with an amended filing at a later date. Filing an electronic return quickly may prevent someone else (who wants to misuse your information) from taking your allocated "slot" in the IRS e-file system.

Q3: What information was compromised/accessed/acquired? Should I be worried about fraud or identity theft?
A3: W-2 forms contain your name, address, Social Security number, income, and all taxes withheld. Law enforcement agencies have indicated that fraud from identity theft can happen very quickly and that W-2s, in particular, have become a major target of cyber attackers who file fraudulent tax returns using your information. You should remain vigilant by reviewing your financial account statements and credit reports for signs of fraud.

Q4: Was my spouse or other family members' information also affected?
A4: No, family members' information was not affected.

Q5: Was there additional information that was compromised – for example, bank accounts?
A5: No, bank account numbers were not exposed, only the information contained on your W-2 form. However, as a precaution, you may want to inform your banks and other financial institutions that your personal information was compromised.

Q6: When did this happen? How did Jenner & Block discover that it happened?
A6: The file was sent on Thursday, February 2, 2017. Jenner & Block management learned of the incident late in the afternoon of February 6, 2017 when the employee realized what had happened and reported the incident.

Q7: What is Jenner & Block doing to address the incident and protect me from fraud or identity theft?
A7: As stated, Jenner & Block is providing all affected employees with complimentary Experian Fraud Resolution assistance and a complimentary two year membership to ProtectMyID® Elite credit monitoring. The fraud resolution assistance is available to you immediately, even if you do not enroll in the credit monitoring service.

Fraud Resolution does not require any action on your part at this time. If, after contacting Experian about an issue that you believe is related to this incident, it is determined that fraud resolution support is needed an Experian Fraud Resolution agent will work with you to investigate and resolve each incident of fraud that occurred from the date of this incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

We are also offering fraud detection tools through ProtectMyID® Elite which does require enrollment, but is of no cost to you and does not require you to provide a credit card or purchase any other products. ProtectMyID® Elite provides you with superior identity detection and resolution of identity theft. Once you enroll in ProtectMyID® Elite you will have access to the following features:

- **Experian credit report at signup:** See what information is associated with your credit file.
- **Active Surveillance Alerts:** Monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet Scan:** Alerts you if your information is found on sites containing compromised data.
- **Address Change Alerts:** Alerts you of changes to your mailing address.

- **Fraud Resolution:** Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- **ExtendCARE**: You receive the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.
- **Lost Wallet Protection:** Get help replacing credit, debit, and medical insurance cards.

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Jenner & Block realizes that dealing with these issues can be time-consuming and frustrating. In the unfortunate event that you need to resolve any fraud or identity theft issues, please take the reasonable time necessary to address the situation during your normal work hours.

Q8: How long should we monitor our credit?
A8: There is no "expiration date" on stolen information, so it is a good idea to review credit reports, bank, credit card and other account statements regularly. Proactively create alerts on credit card and bank accounts for suspicious activity. If unauthorized or suspicious activity is discovered, do not delay! Take action immediately.

Q9: What is Jenner & Block doing to protect my information moving forward?
A9: Jenner & Block has a strong commitment to privacy and data. We are committed to reviewing and refining our procedures and training moving forward.

Q10: Have you notified the police or law enforcement? Has the person who received the information been caught?
A10: The matter has been, and is in the process of being, reported to the IRS, state tax agencies, and to the appropriate law enforcement authorities and government entities in accordance with applicable law. We do not know at this time who the cyber attacker is, or whether she or he will be caught. We are providing via secure transmission the IRS and the state departments of revenue and taxation the affected Social Security numbers (a common practice in this situation).

Q11: Do I need to do anything regarding my taxes or contact the IRS?
A11: Because your W-2 was affected, someone could file a fraudulent tax return using your Social Security number now or in the future.

If you haven't filed taxes for 2016 and no other return has been submitted in your name, the IRS recommends you file your taxes electronically, even if your data is not complete or it contains errors. You can correct any errors in that return with an amended filing at a later date. Filing an electronic return quickly may prevent someone else (who wants to misuse your information) from taking your allocated "slot" in the IRS e-file system.

If you have filed for 2016, you can still submit an IRS Form 14039, Identity Theft Affidavit, in order to protect yourself in the future. If a fraudulent return has been electronically filed in your name, you must:

- File a paper tax return with a completed IRS Form 14039, Identity Theft Affidavit. The IRS recommends that you attach that form to the front of the paper return.
- The IRS has indicated that it may take up to six months to process the valid tax return you filed after a fraudulent return was also filed.

If you try to file your tax return and receive a message that you have already filed for 2016, you should obtain from the IRS an Electronic Filing PIN. The PIN may not protect your 2016 return, but it will provide protection for future filings.

Visit https://www.irs.gov/individuals/get-an-identity-protection-pin or call 800-908-4490 and follow the system prompts. If an accountant or tax preparer files your return on your behalf, he or she may have a PIN for you. Be sure to discuss this incident with your tax preparer.

Q12: Will we receive any additional information or update?
A12: We will continue to communicate with you as appropriate regarding this situation.

Q13: Why didn't you alert me sooner?
A13: We are notifying you as soon as we learned of the situation.

Q14: I'm in the midst of refinancing / buying a home / buying a car, what should I do?
A14: Explain the issue to your bank or financing company, and check your credit report for suspicious activity.

Q15: What happens if my credit is compromised?
A15: If you suspect you are the victim of fraud or identity theft, contact Experian Fraud Resolution at 877-441-6943.

dos.sm.CP.SecurityNotification

From: Callahan, Mary Ellen <MECallahan@jenner.com>
Sent: Thursday, February 09, 2017 8:06 PM
To: 'breach.security@ag.ny.gov'; troopers.sm.ctc.risk.analysis.cell; dos.sm.CP.SecurityNotification
Cc: Callahan, Mary Ellen; Kidwell, Brent E.
Subject: Notification of Unauthorized Access
Attachments: JB W2 Incident NY.AG.pdf; JB W2 Notification Packet.pdf

On behalf of Jenner & Block LLP, enclosed please find notification of unauthorized access of personal information involving New York residents.

If you have questions, please feel free to contact me.

Best,
Mary Ellen

Mary Ellen Callahan

Jenner & Block LLP
1099 New York Avenue, N.W.
Suite 900, Washington, DC 20001-4412 | jenner.com
+1 202 639 6064 | TEL
+1 202 661 4921 | FAX
MECallahan@jenner.com
Download V-Card | View Biography